The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
12/09/2020

SUBJECT:
Multiple Vulnerabilities in Various Opensource TCP/IP Stack Could Allow for Remote Code Execution

OVERVIEW:
Multiple vulnerabilities (known as Amnesia:33) have been discovered in various opensource TCP/IP stacks, the most severe of which could result in remote code execution. As of 2019, a large quantity of embedded projects were found to be utilizing opensource embedded TCP/IP stacks. Successful exploitation of the most severe of these vulnerabilities could allow an attacker to execute remote code in the context of the application or device. Depending on the privileges associated with the application or device, an attacker could install programs; view, change, or delete data; or create new accounts with full user rights. If an application has been configured to have fewer user rights on the system, exploitation of the most severe of these vulnerabilities could have less impact than if it was configured with administrative rights.

THREAT INTELLIGENCE:
There are currently no reports of these vulnerabilities being exploited in the wild. A proof of concept exists for various vulnerabilities mentioned within this advisory. The exploitation showcase within Forescout's research report highlighted CVE-2020-25112 and CVE-2020-24337.

SYSTEMS AFFECTED:
- uIP-Contiki-OS (end-of-life [EOL]), Version 3.0 and prior
- uIP-Contiki-NG, Version 4.5 and prior
- uIP (EOL), Version 1.0 and prior
- open-iscsi, Version 2.1.12 and prior
- picoTCP-NG, Version 1.7.0 and prior
- picoTCP (EOL), Version 1.7.0 and prior
- FNET, Version 4.6.3
- Nut/Net, Version 5.1 and prior

RISK:
Government:
- Large and medium government entities: **High**

- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users: Low

TECHNICAL SUMMARY:

Multiple vulnerabilities (known as Amnesia:33) have been discovered in various opensource TCP/IP stacks, the most severe of which could result in remote code execution. Details of these vulnerabilities are as follows:

Vulnerabilities found in uIP:

- Improper handling of IPv6 extension headers and extension header options and their lengths which may result in an infinite loop. (CVE-2020-13984)
- Improper handling of unsafe integer conversion which may lead to memory corruption. (CVE-2020-13985)
- Improper length checks against decapsulate RPL extension headers which may result in an infinite loop (CVE-2020-13986)
- Improper checks against the length fields of packet headers which may result in an out-of-bound memory read (CVE-2020-13987)
- Improper checks against the length field of the TCP MSS option which may result in an infinite loop (CVE-2020-13988)
- Improper checks against the value of the Urgent data pointer which may lead to memory corruption (CVE-2020-17437)
- Improper checks against lengths and offset in the reassembly of fragmented packets in IPv4 which may lead to memory corruption (CVE-2020-17438)
- A flaw in handling gratuitous DNS replies and the randomness of the DNS transaction ID may allow for DNS cache poisoning (CVE-2020-17439)
- Improper checks against domain names of incoming DNS packets which may result in memory corruption (CVE-2020-17440)
- Improper checks in the process of DNS response handling which may lead to memory corruption (CVE-2020-24334)
- Improper bound checking against the parsing of domain names may lead to memory corruption (CVE-2020-24335)
- Improper checks against the length field of DNS response packets over NAT64 may result in remote code execution (CVE-2020-24336)
- Improper checks for the IPv4/IPv6 header length and the IPv6 header extension lengths may result in remote code execution (CVE-2020-25112)

Vulnerabilities found in picoTCP:

- Improper checks against the payload length field of IPv6 extension headers which may lead to an information leak or denial of service (CVE-2020-17441)
- Improper checks against the length of the Hop-by-Hop extension header may result in an infinite loop which leads to a denial of service (CVE-2020-17442)
- Improper checks against ICMPv6 headers when processing ICMPv6 echo requests may lead to a denial of service (CVE-2020-17443)

- Improper checks against the lengths of extension header options when processing IPv6 headers may result into a denial of service (CVE-2020-17444)
- Improper checks against options lengths when processing the IPv6 Destination Options extension header may result in a denial of service (CVE-2020-17445)
- Improper length validation of TCP options in IPv4 may results in a denial of service (CVE-2020-24337)
- Improper bound checking against the parsing of domain names may result in remote code execution (CVE-2020-24338)
- Improper bound checking against the parsing of domain names may result in a denial of service (CVE-2020-24339)
- Improper checks in the process of DNS response handling which may lead to memory corruption (CVE-2020-24340)
- Improper checks against the length of incoming TCP packets may enable an out-of-bound read and/or memory corruption (CVE-2020-24341)

Vulnerabilities found in FNET:

- Improper checks against domain names when processing LLMNR requests which may lead to an out-of-bound read (CVE-2020-17467)
- Improper checks against the length of the Hop-by-Hop extension header may result in an infinite loop which leads to a denial of service (CVE-2020-17468)
- A memory alignment issue in IPv6 packet reassembly which may result in memory corruption (CVE-2020-17469)
- Lack of randomness in DNS transaction ID which may lead to DNS cache poisoning (CVE-2020-17470)
- Improper checks against domain names from incoming mDNS packets may lead to memory corruption and/or a memory leak (CVE-2020-24383)

Vulnerabilities found in Nut/Net:

- The function in Nut/Net that processes DNS questions/responses has several issues: there is no check on whether a domain name is NULL-terminated; the DNS response data length is not checked (can be set to arbitrary value from a packet); the number of DNS queries/responses (set in DNS header) is not checked against the data present; the length byte of a domain name in a DNS query/response is not checked and is used for internal memory operations. (CVE-2020-25107, CVE-2020-25108, CVE-2020-25109, CVE-2020-25110, CVE-2020-25111)

Successful exploitation of the most severe of these vulnerabilities could allow an attacker to execute remote code in the context of the application or device. Depending on the privileges associated with the application or device, an attacker could install programs; view, change, or delete data; or create new accounts with full user rights. If an application has been configured to have fewer user rights on the system, exploitation of the most severe of these vulnerabilities could have less impact than if it was configured with administrative rights.

RECOMMENDATIONS:

The following actions should be taken:

- All organizations must perform a comprehensive risk assessment before deploying defensive measures.
- First deploy defensive measures in a passive “alert” mode.

- Mitigation for operators and networks:

  (based on CERT/CC and CISA ICS-CERT advisories)
  - Minimize network exposure for all control system devices and/or systems, and ensure that they are not accessible from the Internet.
  - Locate control system networks and remote devices behind firewalls, and isolate them from the business network.
  - When remote access is required, use secure methods, such as Virtual Private Networks (VPNs), recognizing that VPNs may have vulnerabilities and should be updated to the most current version available. Also recognize that VPNs are only as secure as the connected devices.
  - Use an internal DNS server that performs DNS-over-HTTPS for lookups..

- Pre-emptive traffic filtering is an effective technique that can be applied as appropriate to your network environment. Filtering options include:

  - Normalize IP fragments, if IP fragements are not supported in your environment.
  - Disable or block IP tunneling (IPv6-in-IPv4 or IP-in-IP tunneling), if not required.
  - Block IP source routing, and any IPv6 deprecated features, like routing headers VU#267289
  - Enforced TCP inspection, rejecting malformed TCP packets.
  - Block unused ICMP control messages, such as MTU update and Address Mask updates.
  - Normalize DNS through a secure recursive server or DNS inspection firewall. (Verify that your recursive DNS server normalizes requests.)
  - Provide DHCP/DHCPv6 security, with features such as DHCP snooping.
  - Disable/Block IPv6 multicast capabilities if not used in the switching infrastructure.
  - Disable DHCP where static IPs can be used.
  - Employ network IDS and IPS signatures.
  - Employ network segmentation, if available.

REFERENCES:

Forescout:
https://www.forescout.com/company/resources/amnesia33-how-tcp-ip-stacks-breed-critical-vulnerabilities-in-iot-ot-and-it-devices/

ICS-CERT:
https://us-cert.cisa.gov/ics/advisories/icsa-20-343-01

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-13984
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-13985
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-13986
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-13987
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-13988
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-17437
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-17438
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-17439

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-17440
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-24334
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-24335
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-24336
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-25112
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-17441
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-17442
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-17443
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-17444
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-17445
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-24337
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-24338
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-24339
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-24340
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-24341
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-17467
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-17468
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-17469
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-17470
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-24383
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-25107
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-25108
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-25109
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-25110
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-25111